Exponential congruences (Number Theory and its Applications)

AUTHOR(S):

Schinzel, A.

CITATION:

Schinzel, A.. Exponential congruences (Number Theory and its Applications). 数理解析研究所講究録 1998, 1060: 119-123

ISSUE DATE:

1998-08

URL:

http://hdl.handle.net/2433/62367

数理解析研究所講究録
1060 巻 1998 年 119-123

A. Schinzel

Exponential congruences.

Exactly 60 years ago Skolem made a fundamental conjecture about exponential congruences, which runs as follows

Conjecture (Skolem 1937). Let K be a finite extension of $\mathbb{Q}$ and $\beta_{hi} \in K$, $\alpha_{hij} \in K^*$ $(1 \le h \le g, 1 \le i \le l, 1 \le j \le k)$. If the system of congruences

$$\sum_{h=1}^{g} \beta_{hi} \prod_{j=1}^{k} \alpha_{hij}^{x_j} \equiv 0 \pmod{m} \qquad (1 \le i \le l)$$

is solvable for all ideals m of K, then the corresponding system of equations is solvable in integers.

Skolem himself has proved the conjecture for the case $g = 2$, $\alpha_{1ij} = 1$, $\alpha_{2ij} = \alpha_{2j}$ for all i, j. This is a special case of the following

Theorem 1. Let $f_i(z_1, \dots, z_q)$ $(1 \le i \le l)$ be polynomials over K, $\alpha_{pj} \in K^*$ $(1 \le p \le q, 1 \le j \le k)$ and $M \in \mathbb{N} = \{1, 2, \dots\}$. If the system of equations $f_i(z_1, \dots, z_q) = 0$ $(1 \le i \le l)$ has only a finite number of solutions in $\mathbb{C}$ and the system of congruences

$$f_i\Big(\prod_{j=1}^{k} \alpha_{1j}^{x_j}, \dots, \prod_{j=1}^{k} \alpha_{qj}^{x_j}\Big) \equiv 0 \pmod{m}$$

is solvable for all moduli m prime to M, then the corresponding system of equations is solvable in integers.

In some special cases the modulus m can be restricted to prime ideals. Here are ~~two such theorems~~ some such results.

Theorem 2. Let $f \in K[x]$ be of degree d, $\alpha_1, \dots, \alpha_k \in K^*$. If the congruence

$$(*) \qquad f\Big(\prod_{j=1}^{k} \alpha_j^{x_j}\Big) \equiv 0 \pmod{\mathfrak{p}}$$

is solvable for almost all prime ideals $\mathfrak{p}$ of K, then the corresponding equation is solvable in rationals with the least common denominator not exceeding $\max\{1, d-1\}$.

Corollary 1 If $d \neq 2$ solvability of (*) for almost all prime ideals $\mathfrak{p}$ of K implies solvability of the corresponding equation in integers.

For $d = 3$ Corollary 1 fails, as is shown by the following

Example 1 $f(t) = (t-\beta_1)(t-\beta_2)(t-\beta_1\beta_2)$,

where $\beta_1, \beta_2 \in K$ are multiplicatively independent and $\alpha_i = \beta_i^2$ $(i=1,2)$.

Corollary 2. Let $\{F_n\}$ be the Fibonacci sequence. If a congruence

$$F_n \equiv a \pmod{p}$$

is solvable for almost all primes p, then $a = F_k$ with $k \in \mathbb{Z}$.

To deduce Corollary 2 from Theorem 2 one takes $K = \mathbb{Q}(\sqrt{5})$

$$f(t) = (t^2 - a\sqrt{5}t + 1)(t^2 - a\sqrt{5}t - 1), \quad \alpha_1 = \frac{1+\sqrt{5}}{2}.$$

Problem 1. Assume that $F_{3n} \equiv a \pmod{p}$ is solvable for all primes p. Does it follow that $a = F_{3k}$, $k \in \mathbb{Z}$?

Theorem 3 Let $\alpha_{ij}, \beta_i \in K^*$ $(1 \le i \le l, 1 \le j \le k)$ and assume that for at least one i the numbers α_{ij} are multiplicatively independent. If the system of congruences

$$\prod_{j=1}^{k} \alpha_{ij}^{x_j} \equiv \beta_i \pmod{\mathfrak{p}} \qquad (1 \le i \le l)$$

is solvable for almost all prime ideals $\mathfrak{p}$ of K, then the corresponding system of equations is solvable in integers.

Example 2 $K = \mathbb{Q}$, $\alpha_{11} = 2$, $\alpha_{12} = 3$, $\alpha_{13} = 1$, $\beta_1 = 1$

$$\alpha_{21} = 1, \ \alpha_{22} = 2, \ \alpha_{23} = 3, \ \beta_2 = 4$$

shows that the assumption about multiplicative independence in Theorem 3 is necessary even if $\mathfrak{p}$ runs through all prime ideals of K.

Theorem 3 implies the following ~~Corollary~~.

Corollary 3. Let $\alpha_1, \dots, \alpha_l, \beta_1, \dots, \beta_l \in K^*$. If the system of congruences

$$\alpha_i^x \equiv \beta_i \pmod{\mathfrak{p}} \qquad (1 \le i \le l)$$

is solvable for almost all prime ideals $\mathfrak{p}$ of K, then the corresponding ~~equation~~ system of equations is solvable in integers.

In Theorems 2 and 3 and in Corollaries 1,2,3 almost all prime ideals (or primes) means all except a set of Dirichlet's density zero. Then in particular, Corollary 1 implies that if $a, b \in \mathbb{Q}^{\wedge}$ and $b \neq a^k$, then the lower density of primes p such that $p \mid a^n - b$ for some n, is less than 1. Very recently, two Dutch mathematicians P. Horse and P. Stevenhagen have determined exactly the density of such primes, however on the assumption of an extended Riemann hypothesis.

Corollary 3 ~~implies~~ easily implies

Corollary 4 Let $\alpha_1, \ldots, \alpha_l, \beta_1, \ldots, \beta_l \in K^*$, P be the set of prime ideals of K. The implication

$$\overset{\forall}{n_1, \ldots, n_l \in \mathbb{N}} \quad \overset{\dot\forall}{\mathfrak{p} \in P} \quad \mathfrak{p} \mid \alpha_1^{n_1} \ldots \alpha_l^{n_l} - 1 \Longrightarrow \mathfrak{p} \mid \beta_1^{n_1} \ldots \beta_l^{n_l} - 1$$

holds if and only if there exists an integer e such that

$$\beta_i = \alpha_i^e \quad (1 \leq i \leq l).$$

($\overset{\dot\forall}{\mathfrak{p} \in P}$ means „for almost all $\mathfrak{p} \in P$").

A proof appeared recently in volume 2 of Matematicheskiye zapiski dedicated to the memory of N.I. Feldman. The special case $l = 1$ was proved earlier, although published later by C. Corrales-Rodrigáñez and R. Schoof. Now I shall present still unpublished results in the same direction obtained jointly with two French mathematicians, D. Barsky and J.-P. Bézivin. To state these results I need some ~~notation~~.

Notation. Γ_n is the multiplicative group of nth roots of unity.

$\Gamma = \bigcup_{n=1}^{\infty} \Gamma_n$, $\Gamma_w = \Gamma \cap K$.

For a polynomial $F \in K[x_1, \ldots, x_n]$

$$\Omega(F) = \{ \langle \gamma_1, \ldots, \gamma_n \rangle \in \Gamma^n : F(\gamma_1, \ldots, \gamma_n) = 0 \}.$$

Theorem 4 Assume that $R \in K[x_1,\dots,x_r]$, $S \in K[x_1,\dots,x_s]$, $\Omega(R) \neq \emptyset$ and $\Omega(S)$ is finite. Let $\alpha_1,\dots,\alpha_r,\beta_1,\dots,\beta_s \in K^\times$ and $\alpha_1,\dots,\alpha_r$ be multiplicatively independent. If

$$\bigvee_{n\in\mathbb{N}} \overset{\infty}{\bigvee}_{\mathfrak{p}\in P} \mathfrak{p} \mid R(\alpha_1^n,\dots,\alpha_r^n) \Longrightarrow \mathfrak{p} \mid S(\beta_1^n,\dots,\beta_s^n),$$

then there exist integers $e>0$ and d_{ij} such that

$$\beta_i^e = \prod_{j=1}^{r} \alpha_j^{d_{ij}} \qquad (1 \le i \le s).$$

Corollary 5 Let $w=2$ and $\alpha_1,\alpha_2,\beta_1,\beta_2$ be integers of K. Assume that neither $\pm\alpha_i$, nor $\pm\beta_i$ $(i=1,2)$ is a unit or a perfect power in K and that $(\alpha_1,\alpha_2)=(\beta_1,\beta_2)=1$. The implication

$$\mathfrak{p} \mid \alpha_1^n+\alpha_2^n+1 \Longrightarrow \mathfrak{p} \mid \beta_1^n+\beta_2^n+1$$

holds if and only if $\{\beta_1,\beta_2\}=\{\alpha_1,\alpha_2\}$.

The difficult "only if" part of Cor. 5 can be deduced from Theorem 4 as follows. Take $R=S=x_1+x_2+1$. We have $\Omega(R)=\Omega(S)=\{\langle\xi_3,\xi_3^2\rangle,\langle\xi_3^2,\xi_3\rangle\}$, so that the assumption concerning Ω's in Theorem 4 is satisfied. Since α_1,α_2 are integers, different from units and relatively prime, they are multiplicatively independent. Thus Theorem 4 applies and gives

$$\beta_i^e = \alpha_1^{d_{i1}}\alpha_2^{d_{i2}} \qquad (i=1,2)$$

Since also β_i are integers and relatively prime we have either $d_{12}=d_{21}=0$ or $d_{11}=d_{22}=0$. Permuting α_1,α_2, if necessary, we may assume that

$$\beta_i^e = \alpha_i^{d_{ii}} \qquad (i=1,2).$$

Since $w=2$ this equality implies that either one of the numbers $\pm\alpha_i,\pm\beta_i$ is a perfect power in K, or

$$\beta_i = \varepsilon_i \alpha_i \ , \ \varepsilon_i \in \{1,-1\} \ (i=1,2).$$

Now, we take n odd and remember that

$$\mathfrak{p} \mid \alpha_1^n + \alpha_2^n + 1 \Rightarrow \mathfrak{p} \mid \beta_1^n + \beta_2^n + 1.$$

We get

$$\mathfrak{p} \mid \alpha_1^n + \alpha_2^n + 1 \Rightarrow \mathfrak{p} \mid \varepsilon_1 \alpha_1^n + \varepsilon_2 \alpha_2^n + 1.$$

If $(\varepsilon_1, \varepsilon_2) \neq (1,1)$, adding, or subtracting we get $\mathfrak{p} \mid 2\alpha_1^n$, or $\mathfrak{p} \mid 2\alpha_2^n$, or $\mathfrak{p} \mid 2$, which is possible only for finitely many prime ideals $\mathfrak{p}$. Since, by an old theorem of Pólya, there are infinitely many prime ideals $\mathfrak{p}$ dividing $\alpha_1^n + \alpha_2^n + 1$ for some odd n, we infer that $\varepsilon_i = 1$, i.e. $\beta_i = \alpha_i$ $(i=1,2)$.

Corollary 5 suggests the following problems.

Problem 2 Let $\alpha_1, \alpha_2, \beta_1, \beta_2 \in K^*$ and assume that

$$\forall_{n \in \mathbb{N}} \ \forall_{\mathfrak{p} \in P} \ \mathfrak{p} \mid \alpha_1^n + \alpha_2^n + 1 \Leftrightarrow \mathfrak{p} \mid \beta_1^n + \beta_2^n + 1.$$

Is it true that $\{\beta_1, \beta_2\} = \{\alpha_1, \alpha_2\}$ or $\{\alpha_1^{-1}, \alpha_2^{-1}\}$?

The example $\alpha_2 = \alpha_1^2$, $\beta_i = \alpha_i^{-1}$ $(i=1,2)$ shows that the second term of the alternative is really needed.

Problem 3. Disprove the statement

$$\exists_{p_0} \ \forall_{p > p_0} \ \forall_{n \in \mathbb{N}} \ p \mid 2^n - 3 \Leftrightarrow p \mid 5^n - 2.$$

(p prime)

P. Stevenhagen solved Problem 3 assuming an extended Riemann hypothesis.